TURNING DATA INTO ACTIONABLE IN-TELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANA-

CIRCL / TEAM MISP PROJECT



NSPA



Turning data into actionable intelligence

05

2022-08



NSPA

2022-08-05

Turning data into actionable intelligence

└─about CIRCL

circleu
 in the Comparison of the State of the St



The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. CIRCL is the CERT for the private sector, communes and non-governmental entities in Luxembourg and is operated by securitymadein.lu g.i.e.

MISP AND CIRCL

Turning data into actionable intelligence

MISP and CIRCL

2022-08-05

 EIRCL is mandated by the Ministry of Economy and acting as the Luxenburg Mational CERT for private sector.
 EIRCL Leads the development of the Open Source MSP threat Intelligence communities, private companies, fnancial actor, National CER's and LES globally.
 EIRCL nume multiple large MSP communities performing active daily threat-Intelligence sharing.

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing.

THE AIM OF THIS PRESENTATION

Turning data into actionable intelligence

08-05

2022

└─The aim of this presentation

- To give some insight into what sort of an evolution of our various communities' have gone through as observed over the past 8 years
- Show the importance of strong contextualisation...
- _and how that can be leveraged when trying to make or data actionable

- To give some insight into what sort of an evolution of our various communities' have gone through as observed over the past 8 years
- Show the importance of **strong contextualisation**...
- …and how that can be leveraged when trying to make our data actionable

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACK

There are many different types of users of an information sharing platform like MISP:

- Malware reversers willing to share indicators of analysis with respective colleagues.
- Security analysts searching, validating and using indicators in operational security.
- Intelligence analysts gathering information about specific adversary groups.
- Law-enforcement relying on indicators to support or bootstrap their DFIR cases.
- Risk analysis teams willing to know about the new threats, likelyhood and occurences.
- **Fraud analysts** willing to share financial indicators to detect financial frauds.

Turning data into actionable intelligence

Development based on practical user feedback

DEVELOPMENT BASED ON PRACTICAL USER FEEDBACI

- There are many different types of users of an information sharing platform like MISP:
- Malware reversers willing to share indicators of analysis with respective colleagues.
- Security analysts searching, validating and using indicators in operational security.
- Intelligence analysis gathering information about specific adversary groups.
- Law-enforcement relying on indicators to support or bootstrop their DER cacer.
- Risk analysis teams willing to know about the new threats
- Fraud analysts willing to share financial indicators to dete financial frauds.

05

80

2022-

Turning data into actionable intelligence

└─The initial scope of MISP

Extract information during the analysis process
 Store and correlate these datapoints
 Share the data with partners
 Procue on technical indicators: IP, domain, hostname, hashe
 fineame, pattern in file //memory/traffic
 Generate protective signatures out of the data: snort,
 suricata, OpenIOC

- **Extract information** during the analysis process
- Store and **correlate** these datapoints
- **Share** the data with partners
- Focus on technical indicators: IP, domain, hostname, hashes, filename, pattern in file/memory/traffic
- Generate protective signatures out of the data: snort, suricata, OpenIOC

05

8 8 0

2022

INITIAL WORKFLOW



For Turning data into actionable intelligence



WHY WAS IT SO SIMPLISTIC?

က Turning data into actionable intelligence

└─Why was it so simplistic?

- his was both a reflection of our maturity as a community
- Capabilities for extracting information
- Capabilities for utilising the information
 Lack of willingness to share context
- Lack of co-operation between teams doing technical analysis/monitoring and threat-intel
- The more growth we saw in maturity, the more we tried to maturity it with our data and a first surgical and the second state.

- This was both a reflection of our maturity as a community
 - Capabilities for extracting information
 - Capabilities for **utilising** the information
 - Lack of **willingness** to share context
 - Lack of co-operation between teams doing technical analysis/monitoring and threat-intel
- The more growth we saw in maturity, the more we tried to match it with our data-model, often against pushback

8 8

2022-

THE GROWING NEED TO CONTEXTUALISE DATA

2022-08-

05

Turning data into actionable intelligence

└─The growing need to contextualise data

- There were separate factors that made our data-sets less and less useful for detection/defense in general
 Growth of our communities
- Growth of our communities
 Distinguish between information of interest and raw
- False-positive management
- TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
- Increased data volumes leads to be able to prioritise

- There were separate factors that made our data-sets less and less useful for detection/defense in general
 - Growth of our communities
 - Distinguish between information of interest and raw data
 - False-positive management
 - TTPs and aggregate information may be prevalent compared to raw data (risk assessment)
 - Increased data volumes leads to be able to prioritise

OUR INITIAL SOLUTION

2022-08-05

Turning data into actionable intelligence

└─Our initial solution

 Allow users to tag any information created in MISP
 We wanted to be tax with what we accept in terms of data but be strict on what we fed to our tools, with strong filter options

We had some ideas on how to potentially move forward...

Allow users to tag any information created in MISP

- We wanted to be lax with what we accept in terms of data, but be strict on what we fed to our tools, with strong filter options
- We had some ideas on how to potentially move forward...

OUR INITIAL FAILURES

Turning data into actionable intelligence

└─Our initial failures

- Try to capture different aspects of contextualisation into normalised values (threat level, source reliability, etc)
- Don't scale with news coner than our own
 Incorporating new types of contextualisation would mean t
- modification of the software Getting communities with established naming conventions
- use anything but their go-to vocabularies was a pipe-dream Heated arguments over numeric conversions

- Try to capture different aspects of contextualisation into normalised values (threat level, source reliability, etc)
 - Didn't scale with needs other than our own
 - Incorporating new types of contextualisation would mean the modification of the software
 - Getting communities with established naming conventions to use anything but their go-to vocabularies was a pipe-dream
 - Heated arguments over numeric conversions

08-05

2022-

HUMAN CREATIVITY

- We tried an alternate approach instead: Free tagging
 - Result was spectacularly painful, at least 7 different ways to spell tlp:amber
 - No canonisation for common terms lead to tagging ultimately becoming a highly flawed tool for filtering within a sharing community

TLP AMBER		
TLP:AMBER		
Threat tip:Amber		
tlp-amber		
tlp::amber		
tlp:amber		

Turning data into actionable intelligence

Human creativity

08-05

2022

 We tried an alternate approach instead: Free tagging Result was spectravitry painful, at least 7 different ways to spall tipamber No canonisation for common terms lead to tagging ultimately becoming a highly flawed tool for filtering within a sharing community
TLP AMILIE
TLP-AMBOR
Thread By Amber
Ep-celler.
Kg: anber
Ep. soller

HOW WE ENDED UP TACKLING THE ISSUE MORE SUCCESSFULY

- We ended up with a mixed approach, currently implemented by the MISP-taxonomy system
 - Taxonomies are vocabularies of known tags
 - Tags would be in a triple tag format namespace:predicate="value"
 - Create your own taxonomies, recipients should be able to use data you tag with them without knowing it at the first place
 - Avoid any coding, stick to JSON
- Massive success, approaching 100 taxonomies
- Organisations can solve their own issues without having to rely on us

Ta	ag	Events	Attributes	Tags
w	orkflow:state="complete"	11	0	workflow:state="complete"
w	orkflow:state="draft"	0	0	workflow:state="draft"
w	orkflow:state="incomplete"	55	10	workflow:state="incomplete"
w	orkflow:state="ongoing"	0	0	workflow:state="ongoing"

Turning data into actionable intelligence

80

2022-

How we ended up tackling the issue more successfuly

We ended up with a by the MISP-taxono Taxonomies are Tags would be in namespace Create your own data your ag wit Avoid any codin; Massive success, ap Organisations can a rely on us	a mixed appro imy system vocabularies o a triple tag fo predicate="v taxonomies, re h them without g, stick to JSON oproaching to solve their ow	ach, cu f known rmat alue" scipients knowir o taxon n issue	rrently imp tags s should be g it at the f omies s without h	able to use rst place aving to
No.	Cards.	Arritors	Sec.	
workloadine.com/www.			101304104-00	
worklowakie (Instit			workflow states "do	<

WE WERE STILL MISSING SOMETHING...

- Taxonomy tags often non self-explanatory
- Example: universal understanding of tlp:green vs APT 28
- For the latter, a single string was ill-suited
- So we needed something new in addition to taxonomies Galaxies
 - Community driven knowledge-base libraries used as tags
 - Including descriptions, links, synonyms, meta information, etc.
 - Goal was to keep it **simple and make it reusable**
 - Internally it works the exact same way as taxonomies (stick to JSON)

B Ransomv	vare galaxy	
Galaxy ID	373	
Name	Ransomware	
Namespace	misp	
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb21341078	
Description	Ransomware galaxy based on	
Version	4	
Value 4		Synonyms
.CryptoHasYou.		
777		Sevleg
7ev3n		7ev3n-HONE\$T

Turning data into actionable intelligence

2022

└─We were still missing something...

Taxonomy tags often Example: universal u	non self-e nderstandi	xplanatory ng of tip:gree	1 vs APT 28
So we needed somet	hing new in	addition to t	axonomies -
 Community driver Including descript etc. Goal was to keep i Internally it works JSON) 	i knowledge ions, links, s it simple and the exact si	-base tibraries aynonyms, met d make it reusa ame way as tax	used as tags a information, ble onomies (stick to
	\$ Harac	envore gasky	
	has a	11	
	No.	114	
	100	TANK IN ALL IN AN	
	Rarpha	Networks paraphaseter.	
	30		and y

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

2022-08-05

Turning data into actionable intelligence

Broadening the scope of what sort of context we are interested in

BROADENING THE SCOPE OF WHAT SORT OF CONTEXT WE ARE INTERESTED IN

Whe can receive our data? What can they do with it?
 Data accurse, ourser reliability
 Why is this data relevant to out?
 What can be this behind it, what tools were used?
 What sort of mediations are we dealing with? Who are the target?
 What sort dimediates the statist?
 What sort dimediates the data its?

- Who can receive our data? What can they do with it?
- Data accuracy, source reliability
- **Why** is this data relevant to us?
- Who do we think is behind it, what tools were used?
- What sort of motivations are we dealing with? Who are the targets?
- How can we **block/detect/remediate** the attack?
- What sort of **impact** are we dealing with?

PARALLEL TO THE CONTEXTUALISATION EFFORTS: FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared
 Lead to alert-fatigue
- Evaluate engeniestion via out of the
- Exclude organisation xy out of the community?
- False positives are often obvious **can be encoded**
- Warninglist system¹ aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

ld	89	
Name	List of known IPv4 public DNS resolvers	
Description	Event contains one or more public IPv4 DNS resolvers as attribute with an IDS flag set	
Version	20181114	Warning: Potential false positive
Туре	string	
Accepted attribute types	ip-src, ip-dst, domainjip	List of known IPv4 public DNS resolvers
Enabled	Yes (disable)	Ten 1000 website from Move
Values		Top Tooo website from Alexa
1.0.0.1 1.1.1.1 1.11.71.4		List of known google domains

Turning data into actionable intelligence

05

8 8

2022-

Parallel to the contextualisation efforts: False positive handling

PARALLEL TO THE CONTEXTUALISATION EFFORTS: FALS POSITIVE HANDLING

Line quality / false specifier provide motion information being shared
 Locator taker definition
 Locator taker definition

https://github.com/MISP/misp-warninglists

More complex data-structures for a modern age

- Atomic attributes were a great starting point, but lacking in many aspects
- MISP objects² system
 - Simple **templating** approach
 - Use templating to build more complex structures
 - Decouple it from the core, allow users to define their own structures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribute types
 - Allow **relationships** to be built between objects

Turning data into actionable intelligence

More complex data-structures for a modern age

- MORE COMPLEX DATA-STRUCTURES FOR A MODERN AG
- Atomic attributes were a great starting point, but lacking i many aspects
 MISP objects² system
- MISP objects" system
 Simple templating approact
- Use templating to build more complex structures because it from the core allow upper to define.
 - uncouple in from the core, allow users to define their own structures
 MSD cloudd understand the data without includes the
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribut types

^hhttps://github.com/MISP/misp-object

²https://github.com/MISP/misp-objects

05

8 8

2022-

SUPPORTING SPECIFIC DATAMODEL

+		0 ≍	Fit	ers: Al File Network	Financial Proposal	Correlation Warnings	Include deleted attributes	Show context fields	٩		
Date	org c	Calegory	туре	Value		Tags	Galaxies	Comment		Correlate	Related Events
2018-09-28	N F	Name: bark-accou References: 0 🖸									
2018-09-28	c	Dther	status-code: text	A - Active			Add				
2018-09-28	c	Dther	report-code: text	STR Suspicious	Transaction Report		Add				
2018-09-28	c	Diher	personal-account text	type: A - Business			Add				
2018-09-28	P	Inancial fraud	swift: bic	HASEHKHH			Add			2	3849 11320 11584
2018-09-28	F	Financial fraud	account: bank-account-nr	788796894883			Add				
2018-09-28	c	Other	account-name: text	FANY SILU CO.	LIMITED		Add				
2018-09-28	c	Other	currency-code: text	USD			Add				

2022-08-0

പ്പ Turning data into actionable intelligence

└─Supporting specific datamodel

-			144	make make	10.04	
 -	80.10	a later			0	
	-					
	-					
	-	-				
 		-				
		-	>	-		
			X			



37

CONTINUOUS FEEDBACK LOOP

Turning data into actionable intelligence

Continuous feedback loop

- Data ingested by MISP was in a sense frozen in time
 We had a creation data, but lacked a way to use the output
- We had a creation data, but lacked a way to use the output of our detection
- Lead to the introduction of the Sighting system
- The community could sight indicators and convey the time of sighting
- Potentially powerful tool for IoC lifecycle management clumsy query implementation default

- Data ingested by MISP was in a sense frozen in time
- We had a creation data, but lacked a way to use the output of our detection
- Lead to the introduction of the **Sighting system**
- The community could sight indicators and convey the time of sighting
- Potentially powerful tool for IoC lifecycle management, clumsy query implementation default

05

8 8

2022

SUPPORTING SPECIFIC DATAMODEL

Events				
No	Sightings CIRCL: 2	(2017-03-19 16:17:59)		C
No	Inten	(2/0/0)	/	C
No	Inherit	⊪⊘ ⊮⊋ <i>≸</i> (0/ <mark>0</mark> /0)		C
Tags	+			
Date	2016-02-24			
Threat Level	High			
Analysis	Initial			
Distribution	Connected com	munities		
Sighting Details	freetext test			
MISP: 2 CIRCL: 2	4 (2) - restricted	to own organisation only.		

မ္မ Turning data into actionable intelligence

└─Supporting specific datamodel

0	Evens	90		(2017-03-19 1)	117.50)		
		90		(1911)	-	1	
0		90	intest	007			
	Taga Oune Threat Level Analysis Ostribution Sighting Details MSP 2	•	2015-32-34 Figh Initial Commodeat com Replace Accil Mill 4 (2) - NOTICE	mutiko 1 b. ovr. oganisal	04 5HV.		

9

2022-08

MAKING USE OF ALL THIS CONTEXT

2022-08-

05

Turning data into actionable intelligence

└─Making use of all this context

Most obvious goal: Improve the way we query data

- Unified all export APIs
 Incorporate all contextualisation options into API filters
- Incorporate an contextualisation options into API filters
 Allow for an on-demand way of excluding potential false
- Positives
 Allow users to easily build their own export modules feed their various tools

Most obvious goal: Improve the way we query data

- Unified all export APIs
- Incorporate all contextualisation options into API filters
- Allow for an on-demand way of excluding potential false positives
- Allow users to easily **build their own** export modules feed their various tools

EXAMPLE QUERY

/attributes/restSearch

```
"returnFormat": "netfilter",
"enforceWarninglist": 1,
"tags": {
  "NOT":
    "tlp:white",
    "type:OSINT"
  1,
  "OR":
    "misp-galaxy:threat-actor=\"Sofacy\"",
    "misp-galaxy:sector=\"Chemical\""
  ј,
```

Turning data into actionable intelligence

└─Example query

08-05

2022-

tribites/restarch
'retexnformat': "sefficer",
'refered varing(ist': 1,
''refered varing(ist': 1,
''refere: 1
''ype:SBNT'
''minp-galaxy:shreat-actor\'%sfary\''
''minp-galaxy:sector\'Comical\''
1.

SYNCHRONISATION FILTERS

Turning data into actionable intelligence

-Synchronisation filters

- Make decisions on whom to share data with based on
- Context
 MISP by default decides based on the information creator
- decision who data gets shared with Community hosts should be able to act as a safety net for
 - Push filters what can I push?
 - Pull filters what am I interested in?

- Make decisions on whom to share data with based on context
 - MISP by default decides based on the information creator's decision who data gets shared with
 - Community hosts should be able to act as a safety net for sharing
 - Push filters what can I push?
 - Pull filters what am I interested in?
 - **Local tags** allow for information flow control

22

05

80

2022

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

Standardising on high-level TTPs was a solution to a long list of issues

- Adoption was rapid, tools producing ATT&CK data, familiar interface for users
- A much better take on kill-chain phases in general
- Feeds into our filtering and situational awareness needs extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns
 - attck4fraud ³ by Francesco Bigarella from ING
 - **Election guidelines** ⁴ by NIS Cooperation Group

³https://www.misp-project.org/galaxy.html#_attck4fraud ⁴https:

//www.misp-project.org/galaxy.html#_election_guidelines

Turning data into actionable intelligence

8 8

2022

—The emergence of ATT&CK and similar galaxies

THE EMERGENCE OF ATT&CK AND SIMILAR GALAXIES

- Standardising on high-level TTPs was a solution to a long lis of issues
 Adoption was rapid, tools producing ATT&CK data, familiar
- Adoption was rapid, cous producing at reck data, taining interface for users
 A much better take on kill-chain phases in general
- Feeds into our filtering and situational awareness needs
 extremely well
- Gave rise to other, ATT&CK-like systems tackling other concerns

 AttRefraud > by Francesco Bigarella from ING

^{https://www.misp-project.org/galaxy.html#_attck4fraud 'https:} EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

မှု Turning data into actionable intelligence

8 8

2022

Example query to generate ATT&CK heatmaps

/events/restSearc

"returnFormat": "attack",
"tags": [
 "misp-galaxy:sector=\"Chemical\""
],
"timestamp": "16%d"

/events/restSearch

```
"returnFormat": "attack",
"tags": [
    "misp-galaxy:sector=\"Chemical\""
],
"timestamp": "365d"
```

A SAMPLE RESULT FOR THE ABOVE QUERY

မ္မ ကြား Turning data into actionable intelligence

└─A sample result for the above query

100.000	Concession of the	-	1000	-	Province of			-	1010	
		-		or statement	and the second	Repair Chile	Applicate	And a second sec		And in case of the local division of the loc
									Arrist Au	
	in hans									
Statement in the					And the Party of Concession, Name					
	No. No. of	Name of Street, Street								
	4.1.m. (m. p 4.								inclusion.	
00. A A.	are not a					And a second sec			Annual Annual Ver	
	1007									
				-			tion of the local division of the local divi			

Pre Attack - Attack Patter	Enterprise Attack - Att	ack Pattern Mobile Atlack	k - Attack Pattern					0		11 🛛 🖉 🏹 Show al
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Extituation Over Alternative Protocol	Standard Application Layer Protocol
Spearphishing via Service	Command-Line Interface	Login Item	AppCert DLLs	Code Signing	Input Capture	System Network Configuration Discovery	Distributed Component Object Model	Data from Removable Media	Extilization Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Regsvcs/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation for Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Extilitation	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Detense Evasion	Private Keys	Peripheral Device Discovery	Remote Desktop Protocol	Screen Capture	Scheduled Transfer	Remote Access Tools
	Windows Management Instrumentation	LC_LOAD_DYLIB Addition	New Service	Network Share Connection Removal	Brute Force	Account Discovery	Pass the Ticket	Email Collection	Data Encrypted	Uncommonly Used Port
Valid Accounts	Service Execution	LSASS Driver	Sudo Caching	Process Doppelgänging	Password Filter DLL	System Information Discovery	Windows Remote Management	Clipboard Data	Exfiltration Over Other Network Medium	Multilayer Encryption
Supply Chain Compromise	CMSTP	Rc.common	Process Injection	Disabling Security Tools	Two-Factor Authentication Interception	System Network Connections Discovery	Windows Admin Shares	Video Capture	Exfiltration Over Physical Medium	Domain Fronting
Drive-by Compromise	Control Panel Items	Authentication Package	Bypass User Account Control	Timestomp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obluscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modily Registry	Credentials in Files	File and Directory Discovery	Taint Shared Content	Data from Network Shared Drive		Connection Proxy
	Source	Windows Management Instrumentation Event Subscription	Setuid and Setgid	Indicator Removal from Tools	Forced Authentication	Security Software Discovery	Application Deployment Software			Commonly Used Port
	Space after Filename	Change Default File	Launch Daemon	Hidden Window	Keychain	System Service Discovery	Third-party Software	Automated Collection		Data Encoding

2022-08

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



Turning data into actionable intelligence

08-05

Monitor trends outside of MISP (example: dashboard)





DECAYING OF INDICATORS

Turning data into actionable intelligence 05 8 8 2022-

-Decaying of indicators

- · We were still missing a way to use all of these systems in
- Move the decision making from complex filter options t complex decay models
- Decay models would take into account variou sightings, the type of each indicator Sig
- The first iteration of what we have in MISP now took:

- We were still missing a way to use all of these systems in combination to decay indicators
- Move the decision making from complex filter options to complex decay models
- Decay models would take into account various taxonomies, sightings, the type of each indicator Sightings and Creation date
- The first iteration of what we have in MISP now took:
 - 2 years of research
 - 3 published research papers
 - A lot of prototyping

SCORING INDICATORS: OUR SOLUTION

2022-08-05

Turning data into actionable intelligence

└─Scoring Indicators: Our solution

SCORING INDICATORS: OUR SOLUTION

core(streamer) = base_score(streamer, most) + decay(most, st

- Where,
- score ∈ [0, 100]
- base_score ∈ [0, 100] ■ decay is a function defined by model's parame
- decay is a function defined by model's paramet controlling decay speed
- Attribute Contains Attribute's values and metadat
- Model Contains the Model's configuration

Score(Attribute) = base_score(Attribute, Model) • decay(Model, time)

Where,

- **score** \in [0, 100]
- **base_score** \in [0, 100]
- decay is a function defined by model's parameters controlling decay speed
- Attribute Contains Attribute's values and metadata (Taxonomies, Galaxies, ...)
- Model Contains the Model's configuration

IMPLEMENTATION IN MISP: Event/view

= Pivots = Galaxy	+Event graph +Corre	lation graph +ATT&CK mat	trix = Attributes = Discussion										
Galaxies Contractions	(and)										
+ E E	Category Type	Deleted Let Decay score Value Tags	Context 🚏 Related Tags	Filtering tool Galaxies	(1) Comment	Correlate	Related	Feed	DS Distribur	ion Sightings	Activity	Enter value to search Score	Q X Actions
2019-09-12	Network activity ip-src	5.5.5.5 🔇 🕈 🛓 +		8 + 2 +		2	Events	hits) Inherit	ić © ≯ (0100)		NIDS Simple Decaying 65.26 Model 5 79.88	•• •
2019-08-13	Network activity lp-src	8.8.8.8 Sadmiralty-scale Sadmiralty-scale Contention:explo	e:source-reliability="a" x red x 🔄 + 🚨 +	8 + 🛓 +		×	1 2 2 2 Show 11 more	S1:1 (S1:2	inherit	ić © ≯ (500)		NIDS Simple Decaying 54.6 Model 5 52.69	•••
2019-08-13	Network activity lp-src	9.9.9.9 C admiratly-scal C misp:confiden C tip:amber x	e:source-reliability="c" x ce-level="completely-confident" x & + 🞑 +	8 + 🛓 +		8	1 3 19 28 Show 6 more	S1:1 (inherit	心中人 (4/110)	MLL.	NIDS Simple Decaying 37.43 Model 5 0	•• •
2019-08-13	Network activity ip-src	7.7.7.7 3 admirally-scale retention:2d s	e:information-credibility="4" x	8+ ++		8	41	8) Inherit	습 약 🖌 (3/070)	<u> .</u>	NIDS Simple Decaying 37.41 Model 5 0	9 ¥ 8 ¥
2019-07-18	Network activity ip-src	6.6.6.6 🔇 + 🗶 +		⊗ + ≗ +		8	41	8	8 Inherit	ic © ≯ (0000)		NIDS Simple Decaying 23.31 Model 5 0	

Decay score toggle button

Shows Score for each *Models* associated to the *Attribute* type

Turning data into actionable intelligence

2022-08-05

└─Implementation in MISP: Event/view

The second
a new restored of the second s
Section 199
The second of the second secon
The second secon

Decay score toggle button
 Shows Score for each Model's associated to the Attribute type

IMPLEMENTATION IN MISP: API RESULT

```
/attributes/restSearch
"Attribute": [
{
```

```
"category": "Network activity",
"type": "ip-src",
"to ids": true.
"timestamp": "1565703507",
[...]
"value": "8.8.8.8",
"decay score": [
    "score": 54.475223849544456,
    "decayed": false,
    "DecayingModel": {
      "id": "85",
      "name": "NIDS Simple Decaying Model"
```

Turning data into actionable intelligence

05

8 8

2022-

Implementation in MISP: API result

/#tthbusi/station: transport "felow ativity", transport "felow ativity", transport "felow", transport "felow", transport "felow", transport "felow", transport felow, transport felo

IMPLEMENTATION IN MISP: INDEX

Decaying Models

« previous next »

D	Organization	Usable to everyone	Name	Description	Parameters { }	Formula	# Assigned Types	Version	Enabled	Actions
29	1	~	Phishing model	Simple model to rapidly decay phisting website.	{ "iffetime": 3, "idecay, speed": 2.3, "threshold": 30, "default_base_score": 80, "base_score_confg": { restimative- language": 0.5, "phishing": 0.5 } }	Polynomial	9	1	~	■ △ ≘ ♡ Ⅱ
85	1	×	NIDS Simple Decaying Model	Simple decaying model for Network Intrusion Detection System (NDS).	{ "lifetime": 120, "decay_speed": 2, "threshold": 30, "decay_speed": 2, "threshold": 30, "base_score_config": ("astimative- language": 0.25, "priority-level": 0.25, "langeted-threat- indec": 0.125, "false-positive": 0.125 } } }	Polynomial Ø	13	1	~	⊞ & ⊘ II
age 1 of 1	, showing 2 reco	rds out of 2 total, sta	arting on record 1, ending on 2							

View, update, add, create, delete, enable, export, import

Turning data into actionable intelligence

2022-08-05

Implementation in MISP: Index

000	aland M	NOB 05							
-	-	in Teacher	-						
	1.000		840 B	The state	Report O	***	A number of		-
					The second secon				
			T has been been been been been been been bee	ing harpen at the set of the set of the set (as a set of the set (as a set of the set of					
			And the second second						

IMPLEMENTATION IN MISP: FINE TUNING TOOL

II Sho	w All Types B Show MISP Objects	Sean	ch Attribute Type	5	P	alynon	nial		T 0										
	Attribute Type		Category	Nodel ID		100	,												
	aba chi		Financial traud			50	1												
	authentihash	-	Payload delivery			80													
	bank-account-nr		Financial Insud			70													
	bic	۳	Financial Insud			. 60		~											
	bin	•	Financial based			8 50			1	~									
	bro	•	Network activity	10 11		40	1				_								
	bic	•	Financial haud	п		20													
	cc-number	•	Financial haud			10													
0	othash	•	Payload delivery			•	_							20					
0	community-id		Network activity						0.5	10		Days		20	2.5		8.0		
8	domain		Network activity			Lifeti	ime :		-8			days	Expin	atter ölletime	1		1 days a	and 7 hour	
8	domainijo		Network activity	10 84	C	Hecay 1	speed 3	2.3					Score	halved after (1	Half-Me)		0 day an	nd 6 hours	
0	enal-atachment		Payload delivery		CL	toff th	reshold (30											
0	email.dst		Network activity	n		b a da	nd have an		I Int Sime	i Late this root									
8	email.src	*	Payload delivery					C											
8	Siename	*	Payload delivery		Pt	ishing	model		Sim	ple model 6	rapidly d	ecay 🏅	C tak						
	Senarrejau/henthash		Payload delivery		6	AL	wailable r	nodels	0 My mode	is @ Deta	at models								
	Mesarnejimpfuzzy		Payload delivery								Paramete								
	Secure instant	-	Payload delivery				Model	Org	Description	Formeda	Lifetime	Decay	Threshold	Default	Parata		-		
							NUMBER		Description	FORTELES.	Liteure	speco	I Breskees	basescore	Dasescere co	10 0	angs	Whee I	333 KO MC0
•	Network (md5	۳	Payload delivery	13		-	-		frank.	Out-manial				-					
0	Netarajud5 Netarajuhah	1.1	Payload delivery Payload delivery	13 13	×	29	Phishing model	1	Simple model to	Polynomial	3	2.3	30	80	estimative- language	0.5	1	•	

Create, modify, visualise, perform mapping

Turning data into actionable intelligence

2022-08-05

Implementation in MISP: Fine tuning tool



IMPLEMENTATION IN MISP: base_score TOOL

Search Taxonomy	×	3 not hav	ing numerical value		admirally-scale information-credibility (20%)	priority-	level (45%)	
Default basescore 80								
Taxonomies	Weight							
admiralty-scale 🕶								
source-reliability -			31					
information-credibility -			30					
priority-level -								
priority-level -		3	53		admiraky-scale:source-reliability (27%)			
retention *								
retention -	8		0					
estimative-language -								
likelihood-probability -	1		0					
confidence-In-analytic-judgment -			0					
misp ~								
confidence-level -	8		0					
threat-level -	8		0		Placeholder for 'Organisation	source confidence		
automation-level -	8		0	Example	ø			
phishing -								Base
state -	8		0	Tag your	Tags			score
psychological-acceptability -	8		0	attribute	-			
Excluded •		_		Attribute 1	admiralty-scale:information-credibility="5"			0.0
				Attribute 2	priority-level:baseline-minor admiralty-sca admiralty-scale:information-credibility="2"	ile:source-reliability="d"		38.2 😡
				Attribute 3	priority-level:severe admiralty-scale:inform	nation-credibility="2"		84.6 😧
				Computa	ation steps			
						Computat	ion	
				Tag		Eff.		Result
						Ratio	Value	44.00
				priority-lev	er.baseline-minor	0.46 *	25.00	11.62
				admiralty-	scale:source-reliability="d"	0.27 *	25.00	6.80

പ്പ Turning data into actionable intelligence

LImplementation in MISP: base_score tool



2022-08

IMPLEMENTATION IN MISP: SIMULATION TOOL

Turning data into actionable intelligence

Implementation in MISP: simulation tool



 Base score [] Base score configuration not set. But default value sets. NIDS Simple Decaying Mode RestSearch Specific ID Computation Result CH. Attribute RestSearch⁶ Ratio Value × 75.00 "includeDecayScore": 1, "includeFullModel": 0. × 50.00 0 "score": 30, × 100.00 0 "decayingModel": [85], 0 × NoN 0 "to_ids": 1, "tags": l'estimative-language%", "prioritybase score 80.00 September Sighting Wed Sep 4 12:18:09 2019 Current score 54:60 August October November December Event Teen Galaxies × NIDS Simple Decaying ... 37.41 ORGNAME Network activity ip-sro 8888 admiralty-scales V III NIDS Simple Decaying ... 54.6 Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

Simulate Attributes with different Models

08-05

2022

IMPLEMENTATION IN MISP: API QUERY BODY

/attributes/restSearch

```
"includeDecayScore": 1,
"includeFullModel": 0,
"excludeDecayed": 0,
"decayingModel": [85],
"modelOverrides": {
    "threshold": 30
}
"score": 30,
```

Turning data into actionable intelligence

Implementation in MISP: API query body

IMPLEMENTATION IN MISP: API QUERY BODY

attributes/restSearch

"includeDecayScore": 1, "includeFullModel": 0, "excludeDecayed": 0, "decayingModel": [85], "modelOverrides": ["threshold": 30] "score": 30,

2022-08-05

TO SUM IT ALL UP...

Turning data into actionable intelligence

└─To sum it all up...

05

80

2022-

- Massive rise in user capabilities
- Growing need for truly actionable threat intel
 Lessons learned:
- Context is king Enables better decision making
 Intelligence and situational awareness are natural
 - by-products of context
- Don't lock users into your workflows, build tools that enable theirs

Massive rise in user capabilities

Growing need for truly actionable threat intel

Lessons learned:

- **Context is king** Enables better decision making
- Intelligence and situational awareness are natural by-products of context
- Don't lock users into your workflows, build tools that enable theirs

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

Turning data into actionable intelligence

-Get in touch if you have any questions

GET IN TOUCH IF YOU HAVE ANY QUESTION

Contact us

- https://twitter.com/mokaddem_sa
- https://twitter.com/igte
 Contact CIRCL
- ► info@circLiu
- https://twitter.com/circl_1 https://www.circl_1u/
- Contact MISPProject
- https://github.com/MISP
- https://gitter.im/MISP/MISP
 https://twitter.com/MISPProje

Contact us

- https://twitter.com/mokaddem_sami
- https://twitter.com/iglocska

Contact CIRCL

- ▶ info@circl.lu
- https://twitter.com/circl_lu
- https://www.circl.lu/

Contact MISPProject

- https://github.com/MISP
- https://gitter.im/MISP/MISP
- https://twitter.com/MISPProject

05

80

2022